Analysis of Cloud Computing Information Security Strategy in Biznet Networks

Heri Sutrisno

Electrical Engineering, Mercu Buana University
Jakarta-Indonesia
Email: herisutrisno@gmail.com

Abstract- Information security on cloud computing requires good planning and understanding of the risks, threats and vulnerabilities of data or information that is managed in a cloud computing environment. Measurement of information security in cloud computing is no different to conventional information technology, which uses an approach based on confidentiality, integrity and availability of information. Whereas the standard used on information security such as NIST, CSA and COBIT are often used to assess information security analysis of the cloud computing service providers. This research will review the information security strategy at Biznet Networks as a provider of cloud computing services.

Keywords: *Cloud Computing, Cloud Computing Architecture, Cloud Computing Security, information security strategy*

1. INTRODUCTION

Cloud computing has the potential to provide a variety of innovative services for infrastructure management, application development platforms and software applications as well as complex business processes to be more efficient and effective when compared to conventional services on information technology. Information security strategy is necessary as mobilization efforts and guidance technology to achieve the goals of information security are confidentiality, integrity and availability of the information. To fulfill challenges of the security information, required the strategy based on internal and external factors as the company's cloud computing service providers in order to fulfill information security goals.

There is a definition of cloud computing by NIST (National Institute of Standards and Technology) is defined as follows: *"Cloud Computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*[8].

2. CLOUD COMPUTING ISSUES

Can be identified that the threat to the security and privacy of cloud computing services is a problem that needs to be considered for service users[11]. Information security issues in cloud computing is a common problem for all cloud services. So that the problem will be analyzed in this research are as follows: *"What is the information security strategy that can be guarantee the confidentiality, integrity and availability of information on cloud computing services at Biznet Networks ?"*

3. INFORMATION SECURITY MEASUREMENT

NIST (National Institute of Standards and Technology) [7] has defined three information security measurement principles, namely confidentiality, integrity and availability of the implementation can be described as follows:

Implementation of *"Confidentiality"* on cloud computing services relating to privacy and to mitigate threats or disturbances can be done by:

1. Access Control, by controlling access to information and what information can be accessed. Could use a password and biometric authentication.
2. Passwords, an authentication method for a more secure basis and be able to use biometrics or smart cards.
3. Biometric, used in human physical characteristics for identification and authentication, for example finger print scan, retina scan or face scan.
4. Encryption, to encrypt information from plain text so it can not be read and will avoid unauthorized users to access information.
5. Ethics, by policy employees as a reference for behavior and prevent the use of inappropriate related information systems.

Implementation of the *"Integrity"* of information on cloud computing services can be implemented through:

1. Configuration Management, how to manage the changes in the IT environment
2. Configuration Audit, control mechanisms to modified and the information allowed to be changed. Results can be monitored by the audit log that stores information changes manually or automatically through the system

Implementation of *"Availability"* on cloud computing services are used to ensure users are entitled to access information anytime and ensure the following actions performed:

1. Data Backup Plan, have a backup plan related information is very important there. Including what information you want to backup and when
2. Disaster Recovery Plan (DRP), including procedures to perform backups and minimum impact on the business
3. Business Continuity Plan (BCP), about how to restore the normal condition after disruption

4. ABOUT BIZNET NETWORKS

Biznet Networks [19] was established in 2000 with a focus on the corporate market. Biznet owns and operates cutting-edge fiber optic network with the largest data center in Indonesia, and also has been providing premium service with fast performance and reliable network. Biznet Networks is also a provider of fixed-line telecommunications and multimedia provider in Indonesia that provides network services (network), Internet services, data centers, as well as hosting and cloud computing services. Biznet Cloud Computing platform provides several options including the processor, memory size, storage (hard disk) and various types of Operating System. The platform also automatically perform load balancing so able to deliver maximum application. Here is a service cloud computing provided by Biznet:

1. Cloud Hosting - provide Cloud Servers services with a larger storage capacity, software applications are like web databases, control panel.
2. Cloud Server - provides the ability to computerize the process with multiple processor options.
3. Cloud Storage - provides online storage space for backup files safely.

5. RESEARCH MEASUREMENT METHODOLOGY

The data used in this research comes from two sources, namely external data through an online questionnaire method and data from internal conducted through questionnaires and interviews to gather information. The following is a chart of the process of measurement and data analysis. In Figure 1, illustrated that the source of the data used in this research is obtained from external data and internal data, with the following explanation;

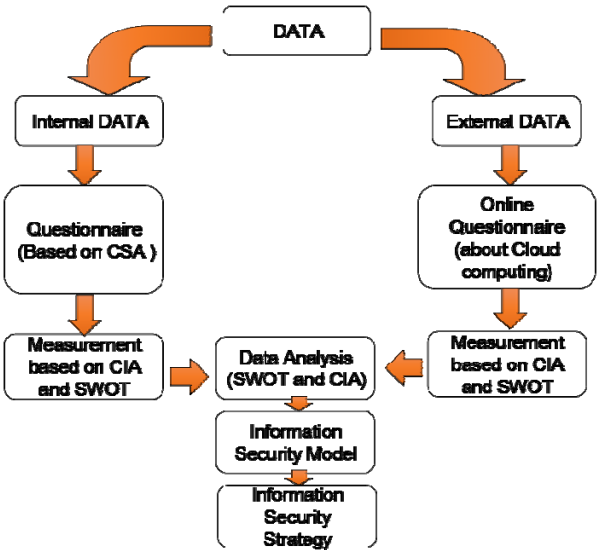

Figure 1. Processes and analysis data

1. External data is data or information obtained from responses to questionnaires that promoted online to the general public through IT mailing list or email. External data is intended to determine the response to the security of cloud computing users.
2. Internal data in this research is obtained from responses to questionnaires by Biznet Networks' management of information security model based on cloud computing made by the CSA (Cloud Security Alliance).

6. ANALYSIS OF THE DATA

The results of external and internal data be analyzed to determine the score of each of the results obtained. The measurement results will be analyzed based on SWOT and the measurement of the CIA (Confidentiality, Integrity, Availability), except for the internal data plus assessment with COBIT 4.1

6.1. External Data

The objective of external data is to find understanding and consideration faced by users / potential users and user expectations for cloud computing security. General information about the correspondents who followed the online questionnaire is as follows:

Table 1. General information of respondents

No	Description	Total
1	Number of respondents	60
2	Already know about cloud computing	76.69 %
3	Which has a number of IT employees as much as 1 up to 50 people	62.50%

The results of the calculation of the "Opportunities" and "Threats" according to the respondents are as follows:

Table 2. Assessment of the "Opportunities"

No	OPPORTUNITIES	%
1	The public has to know about cloud computing	76.69 %
2	The benefits of cloud computing services more than the risk	57.81 %
3	Favorite type of service is IaaS	47.37 %
4	Hardware and Software cost savings and operational information technology, is considered using cloud services	37.67 %
5	Cloud computing services can be accessed from anywhere	15.75 %
6	Data Backup guarantees on Cloud	13.01

	computing solutions	%
7	Business and users can focus on their main business companies	10.27 %

Table 3. Assessment of the "Threats"

No	THREATS	%
1	Do not believe the security of corporate data managed in cloud computing	23.44 %
2	Public concerned with the risk of data leakage	22.66 %
3	Public concerned with data security, privacy and integrity	20.39 %
4	Unauthorized access to the data	14.84 %
5	System integration with internal applications provided by cloud providers	14.79 %
6	The risk of availability of services	13.28 %
7	Network Access Control Security	11.84 %

While the results of consideration correspondent for the CIA (Confidentiality, Integrity and Availability) are as follows.

Table 4. Assessment of the "CIA"

No	CONFIDENTIALITY	%
Consideration prior to the adoption of cloud computing services		
1	Security of information stored in cloud computing	19.72%
2	Can not control the data or information stored in the cloud computing	10.56%
Information security risks		
1	Lose of control	
2	Unauthorized access to information in cloud computing	14.84%
INTEGRITY		
Consideration prior to the adoption of cloud computing services		
1	Integrity with existing internal systems	14.79%
Information security risks		
1	The risk of data leakage in cloud computing	22.66%
2	Privacy and integrity	20.29%
3	Cloud Computing Governance	11.18%
AVAILABILITY		
Consideration prior to the adoption of cloud computing services		

1	Disaster recovery and business continuity of the CSP	12.68%
Information security risks		
1	Business continuity risks in cloud computing services	13.28%
2	Disaster recovery against the information stored in the cloud computing	11.84%

6.1.1. Analysis of the "Opportunities"

In general, the public has to know basic information about cloud computing (79.69%) from a variety of sources, although not all decide to use cloud computing services. With a cloud solution, more perceived benefits gained by society or the company (57.81%) as against the expenditure cost savings of hardware and software (21:23%) compared with the potential risks involved in cloud computing services. IaaS (Infrastructure as a Service) is a solution of the most desirable models (47.37%) by the user because they can save on capital expenses and maintenance of the hardware and software.

6.1.2. Analysis of the "Threats"

Confidence in the security of information (23:44%) were managed in the cloud computing into consideration for the user to initiate the adoption of cloud services solutions. And security of data stored in the cloud computing a concern because the user can not control directly (10:56%). The data transmitted, processed or stored in the cloud can increase the likelihood of threats such as data leakage (22.66%), the privacy and integrity of data (20.39%) is caused by the other party either intentionally or unintentionally.

6.1.3. Analysis of the "Confidentiality"

Information security in cloud computing, a major consideration for the people (19.72%) before to adopt cloud computing services. With services that are controlled by third parties, perceived by users as losing full control (10:56%) to their data stored in cloud computing, as well as access to the data (14.84%) is also a possible risk opportunities.

6.1.4. Analysis of the "Integrity"

Therefore, not all applications will use the company's cloud computing service, the integrity between applications or systems that are run internally by companies and are run in cloud computing (14.79%) into consideration prior to the adoption of cloud computing services. The data stored in the cloud computing has the risk of data leakage (22.66%) were performed by other tenants (multi-tenant), internal party Biznet Networks or interference from outside.

Hence the need of good governance (11:18%) such as policies and procedures governing the operation of cloud computing.

6.1.5. Analysis of the "Availability"

The continuity of services by Biznet Networks of public concern or enterprise, especially against their data. If disaster strikes (12.68%), the need for strategy or actual steps of the Biznet Networks to ensure that the data or company information that is stored and processed in the cloud services they can take place without any hindrance or interference. Biznet Networks required to convince users that they already have a disaster recovery plan (DRP - Disaster Recovery Plan) and also has the operational backup solution (DRC - Disaster Recovery Center). So as to ensure continuity of business customers (13.28%).

6.2. Internal Data

The objective of internal data is to determine the readiness of the Biznet Networks in anticipation of vulnerability, risk and risk mitigation for the delivery of cloud computing.

6.2.1. Assessment of the "Strength" and "Weakness"

An assessment of the internal questionnaire based on strength and weakness are as follows.

Table 5. Assessment of the "Strength" and "Weakness"

No	STRENGTH
1	Planning of network penetration testing has documented and performed regularly
2	Having control and secure data removal procedures
3	Have security policies and procedures working environment equipped with electronic surveillance
4	Employment agreements and employment contracts of employees and contractors are in compliance with existing regulations
5	Employees have been trained and follow procedures in the event of termination of employment
6	Scan network-layer has been carried out periodically
7	Has a policy of sanctions against violations of security policies and procedures
8	Have anti-malware program for all systems
9	Have the incident management system and monitoring its impact
10	BC and DR programs have documented
11	Location of the data center is located in a safe environment and equipment protection mechanism has been implemented

12	Has been the implementation of the ISO 27001 information security standard
WEAKNESS	
1	IT Audit report results can not be read by tenants
2	Not have policies and procedures for the protection of intellectual tenants
3	Tenants do not have the right to determine the geographical location of data storage
4	There is no activity on the vulnerability scan application-layer periodically
5	There are no events scans the operating system - layer periodically
6	Does not have a conflict of interest policies for tenants
7	Have not done a risk assessment on a regular basis
8	Tenants do not know of any BC and CP
9	Result in achievement of SLA is not distributed to tenants

6.2.1.1. Analysis of the “Strength”

Biznet Networks has established policies and procedures related to data management and contract employees or third parties working with Biznet Network already has a contract to support the cloud computing services. Precautions against virus threats from the outside has been overcome by having an anti-malware application. To support continuity of operations, has had a program Biznet Network Business Continuity and Disaster Recovery are documented. Currently have policies regarding intellectual property rights tenants and have implemented information security standards such as ISO 27xxx.

6.2.1.2. Analysis of the “Weakness”

The results of audit and information security systems have not been or are not published to the public, so that people do not know Biznet Network readiness in anticipation of security information on cloud computing services. As well as the vulnerability scan has not been implemented at the application layer and the operating system on a regular basis. SLA achievement results have not been presented to the user to demonstrate the achievement of each parameter in SLA.

6.2.2. Assessment of the “CIA”

The total result is based on an assessment of the internal questionnaire CIA (Confidentiality, Integrity, Availability) using supervisory control CSA (Cloud Security Alliance) is as follows.

Table 6. Assessment of the "CIA”

No	Criteria	Have	Not have
1	Confidentiality	25%	7%
2	Integrity	44%	6%
3	Availability	31%	6%
Total		81%	19%

While the summary of the assessment for each supervisory control used by CSA as follows.

Table 7. Assessment for supervisory control

No	Supervisory Control	Confidentiality	Integrity	Availability	No of questions
1	Compliance	13%	25%	38%	8
2	Data Governance	33%	22%	22%	9
3	Facility Security	29%	14%	29%	7
4	HR Security	25%	50%	25%	4
5	Information Security	26%	22%	39%	23
6	Risk Management	25%	25%	25%	4
7	Resiliency	17%	17%	33%	5
8	Security Architecture	33%	33%	17%	6

6.2.2.1. Analysis of the “Confidentiality, Integrity and Availability”

In general, Biznet Networks has been implementing rules or oversight of information security based on three (3) measurement and has a value of 81%. Achievement level of implementation of the confidentiality of data or information within the Biznet Networks acquire 25% of the total 81%. This show is still a need to increase the confidentiality of data or information, and disclosure of information to the user as well as the geographical place of data storage.

Biznet Networks do not have policies and procedures to protect intellectual property. To ensure data security, technical control has been implemented as the implementation of data management policies and procedures. And supported by operating physical facilities are protected and monitored to avoid unauthorized access. Labor operations have been performed validation runs background to ensure compliance and security of data or information, and conducted surveillance of access that is no longer valid.

To ensure the integrity of data and information, Biznet Networks has conducted one of the control audit by internal and external parties, although not yet submitted the results to the public. To ensure that unauthorized access and changes to data as in a state of in-transit, or not in use encryption step has been done. To ensure availability of services and information, the anticipatory measures such as BCP has been done and tested to anticipate the disaster and

recovery process (recovery) effectively. The process of data backup with the proper procedures have been delivered to customers and verifiable. Every incident of the service is managed by the management of incidents and communicated to tenants including restoration measures, although the total achievement of SLA has not been delivered to the tenants.

7. INFORMATION SECURITY MODEL

Based on the analysis of research data, the model can be made that the information security controls based on risk. Risks that arise depending on the services provided by the Cloud Service Provider (CSP), In Figure 2 describes the information security model based on risk, control and risk mitigation.

The basic principle of information security are Confidentiality, Integrity and Availability as described previously. To realize the security controls necessary information so as to protect the security layer in cloud computing environments. Users or customers with all kinds of equipment used trying to make access to information assets such as data and applications through a process that has been designed previously. Access to information assets proficiency level can occur through the Internet connection of external infrastructure such as CSP or from internal LAN through that of the CSP environment itself so necessary risk controls to ensure there are no violations. Based on these risks, it is necessary to minimize the supervision or control of an incident or problem and to measure the level of risk.

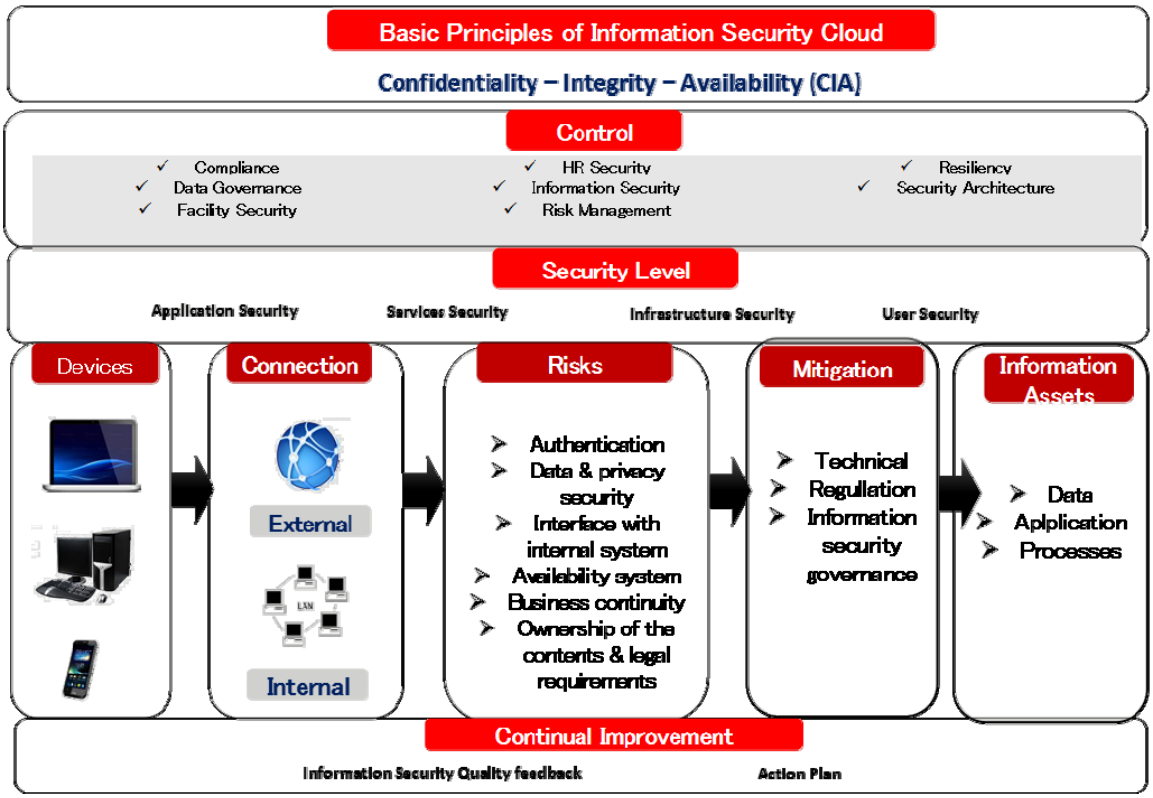

Figure 2. Information Security Model of Cloud Computing

The control needs to be done to mitigate the risks, so as to reduce the risk of impact or even avoid the risk not to happen. Mitigation measures to protect the information assets that include data, applications and processes in a cloud computing environment. Continuous improvement (Continual Improvement) was to always make improvements to the results of the implementation of information security controls based on the results obtained from unpan behind dinyatakn information security and the corrective action plan in accordance with the priorities

8. PROPOSED INFORMATION SECURITY STRATEGY

Based on the research results, the proposed Cloud Computing information security strategies are divided into 2 groups:

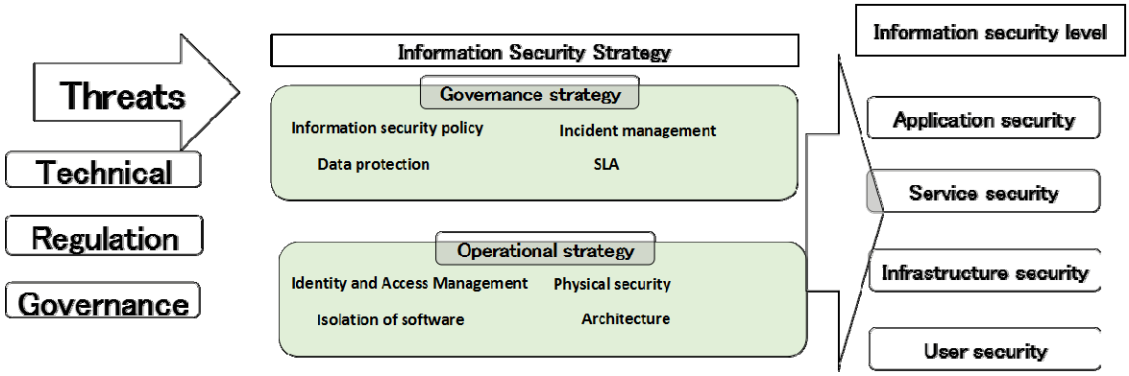

Figure 3. Information Security Strategy

8.1. Governance Strategy

Governance strategy involves monitoring through policies, procedures and standards used for application development, including the design, implementation, testing and monitoring of services provided to customers.

Information Security Policy

Objective-information or data belonging to customers (tenants) have guaranteed the confidentiality, integrity and availability. By keeping the information resource can be avoided the risk of theft, misuse and destruction of data or information. In order to ensure the security of information, necessary to establish responsibility and responsible for security of information so as to continue the activities of Cloud Computing services if an incident occurs.

Data Protection

Objective-data stored in the CSP environment guaranteed by the law relating to the location of data storage and data ownership statement.

Incident Management

Objective-responses to incidents in the cloud environment.

Service Level Agreement (SLA)

Objective-contract between the CSP and the customer to a specific period and to ensure service and warranty provided by the CSP according to the size of the collective agreement.

8.2. Operational Strategy

Operational strategies include access to information assets by tenants or other parties, and also ensure the confidentiality and integrity of applications in cloud computing services, physical security on the CSP environment and architecture of cloud services provided by the CSP to run a Cloud Computing service operations.

Identity and Access Management (IAM)

Objective-maintain the data or sensitive information and privacy against unauthorized access by running the authentication system.

Isolation of Software

Objective-to make sure the software is used for a particular tenant will be isolated and protected to avoid disclosure, theft of information by other parties who are not entitled to*Physical Security*

Objective-protecting information assets against physical destruction or unauthorized access and physical access by employees CSP

Architecture

Objective-protecting cloud services to ensure the reliability and scalability

9. CONCLUSION

Analysis of information security strategy at Biznet Network as a service provider in terms of three (3) criteria: Confidentiality, Integrity and Availability (CIA) to consider internal and external parties can be presented as follows. Measurements show the maturity level of process maturity level is in the range:

'Defined' (Score 3 on Optimum scale of 5)

At this level of information security maturity is generally described as:

"It has been proven that the information security strategy Netwotks Biznet has had a policy process and procedures to ensure the confidentiality, integrity and availability of data or information. Continuity of service has been planned and on the run are listed on BCP and DRP. Communication about the success rate of security-related services in particular need information presented to the user to improve confidence. In general, the information security of cloud computing services Biznet Networks is carried out in an organized manner "

References

[1] Anthony Bisong, Syed (Shawon) M. Rahman (2011), an overview of the security concerns in enterprise cloud computing, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011, Ph.D. Student, Capella University 225 South 6th Street, 9th Floor Minneapolis, MN 55402, USA

[2] Rohit Bhadauria & Sugata Sanyal, Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques, International Journal of Computer Applications (0975-880), Volume 47-No.18 June 2012. School of Electronics and Communications Engineering, Vellore, India

[3] Cloud Security Alliance (2011), security guidance for critical areas of focus in cloud computing v3.0

[4] ISACA (2011), Security consideration for Cloud computing, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA, Web site: *www.isaca.org*

[5] ISACA (2011), Cloud Computing Management Audit/Assurance Program, 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA, Web site: *www.isaca.org*

[6] NIST (2011), Guidelines on security and privacy in public cloud computing

[7] National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995.

[8] NIST (2011), NIST Cloud Computing Standards Roadmap (NIST CCSRWG-092), First edition, July 5, 2011

[9] Erick A. Marks / Bob Lozano (2010). Executive's Guide to Cloud Computing. John Wiley & Sons, Inc., Hoboken, New Jersey.

[10] Borco Furht / Armando Escalante (2010). Handbook of Cloud Computing. Springer New York Dordrecht Heidelberg London.

[11]www.gartner.com;http://blogs.gartner.com/neil_macdonald/2010/12/16/securit-is-the-top-concern-for-public-cloud-but-what-does-that-really-mean/

[12] KPMG International (2011), "Clarity in the Cloud", publication date November 2011, publication number : 111028; http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cloud-clarity.pdf

[13] National Institute of Standards and Technology. "An Introduction to Computer Security: The NIST Handbook." Special Publication 800-12. October 1995.

[14] Cloud Security Alliance (CSA); Consensus Assessments Initiative Questionnaire v1.1 (CSA-CAI-Question-Set-v1-1_FINAL_v6.xls)

[15] Cloud Security Alliance-CSA, "Cloud Controls Matrix (CCM)" at http://www.cloudsecurityalliance.org

[16] The IT Governance Institute (ITGITM) (*www.itgi.org*), COBIT 4.1, IT Governance Institute 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA

[17] Key Management Models, 2nd edition, Marcel van Assen, Gerben van den Berg and Paul Pietersma

[18] http://www.hukumonline.com, Jumat, 5 Juli 2013, Teguh Arifiyadi, S.H., M.H.

[19] www.biznetnetworks.com